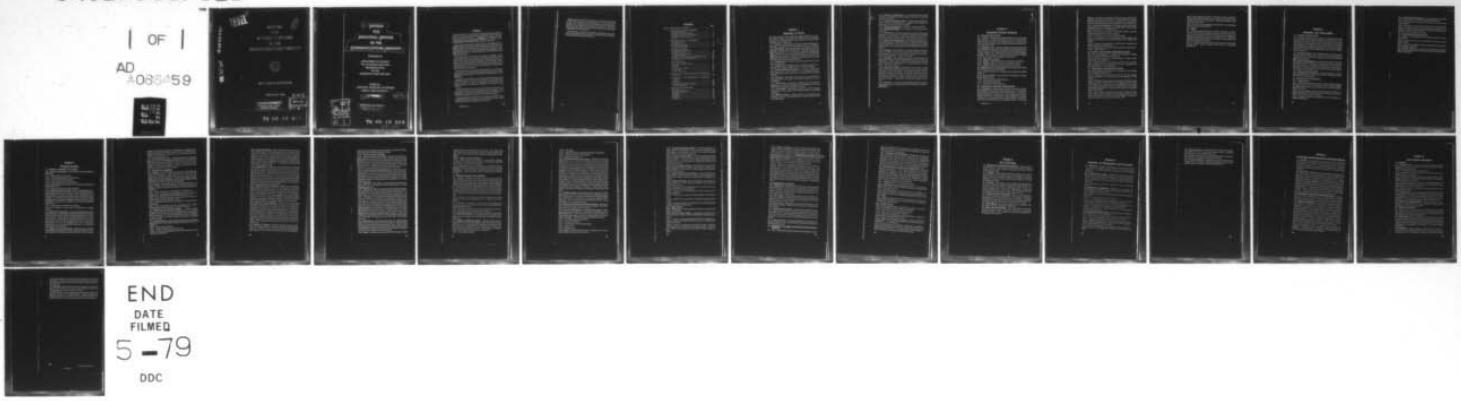
AD-A066 459 DEPARTMENT OF DEFENSE WASHINGTON D C F/G 15/3
CRITERIA FOR INDUSTRIAL DEFENSE IN THE COMMUNICATIONS INDUSTRY.(U)
NOV 60

UNCLASSIFIED NL

| OF |
AD A066459



END
DATE FILMED
5-79
DDC

CRITERIA FOR INDUSTRIAL DEFENSE IN THE COMMUNICATIONS INDUSTRY

DEPARTMENT OF DEFENSE

NOVEMBER 1960

(6)

CRITERIA FOR INDUSTRIAL DEFENSE IN THE COMMUNICATIONS INDUSTRY

PREPARED BY

DEPARTMENT OF DEFENSE
IN COLLABORATION WITH
REPRESENTATIVES
OF THE
COMMUNICATION INDUSTRY

ISSUED BY
ASSISTANT SECRETARY OF DEFENSE
(SUPPLY AND LOGISTICS)

(11) NOV [redacted] 60

(12) 27 p.

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

Preface

This publication is concerned with the industrial defense of facilities within the communications industry, particularly those which are vital to industrial mobilization. It supersedes the material contained in "Standards for Plant Protection," Department of Defense, 1 June 1952, insofar as the communications industry is concerned.

These Criteria have been developed jointly by representatives of the Department of Defense and representatives of the communications industry and are specially tailored to be used for that portion of the communications industry which comes under the provisions of the Armed Forces Industrial Defense Regulation, dated September 1960, or revisions thereof.

The application of these Criteria by industry is desirable. These Criteria are intended as material for the guidance of both government representatives and company management in appraising the status of security of key communications facilities. The acceptance of such criteria by the industry does not imply a commitment to implement the features included in such criteria, or the recommendations submitted by government representatives.

These Criteria have been specifically designed for use with Department of Defense Industrial Defense Survey Forms, DD 395–2 "Communication Company Report" and DD 395–3 "Communication Facility Survey."

The material assembled herein reflects the current doctrine of the Industrial Facilities Protection Branch, Office of the Assistant Secretary of Defense for Supply and Logistics, as influenced by established practices in the field, and as applicable to the communications industry.

Where additional data concerning these Criteria are desired on the part of the communications management, such information, advice and guidance will be furnished through local industrial defense survey personnel of the agency assigned industrial defense cognizance.

The necessity for the entire plan or any portion thereof as encompassed by the Criteria is subject to review at any time at the instance of either industry or the Department of Defense.

574605—60——1

The protection of classified information in the hands of industry covered in the industrial security program, is not covered in this manual. The Department of Defense publication, "Industrial Security Manual for Safeguarding Classified Information," dated June 1960, or revisions thereof, establishes procedures for the safeguarding of classified Defense information.

The Department of Defense gratefully acknowledges the assistance of the communications industry in contributing time and experience to the development of these Criteria.

Contents

Section 1

Definition of Terms

1.1 The definitions as set forth below apply specifically to industrial defense within the communications industry. Their application to matters of industrial defense is governed by the Armed Forces Industrial Defense Regulation.

1.1.1 **Facility.** Any physical plant location, including buildings and equipment. (This term is not to be confused with wire facilities.)

1.1.2 **Key Facility.** Any physical plant location included in the Department of Defense Key Facilities List. The Department of Defense Key Facilities List is composed of selected manufacturing plants, utilities and services, and government-owned installations, which are located within continental United States, and which are of outstanding importance in support of military operations or military production and mobilization programs.

1.1.3 **Company Level.** The top management organization of a company or corporation.

1.1.4 **Facility Level.** Management at the facility designated as responsible for industrial defense coordination at the facility.

1.1.5 **Industrial Defense Coordinator.** An employee designated at the company level or at the facility level as responsible for planning, coordinating, and directing or supervising industrial defense activities.

1.1.6 **Criticality.** The degree of importance of one operating or servicing function of a facility to the overall operations or services of a facility.

1.1.7 **Critical Area.** An area of a facility vital to the functions, operations, or services of the facility, which if damaged or destroyed would disrupt essential communication service.

1.1.8 **Vulnerability.** Vulnerability is the degree to which any given critical area within a facility, or the facility as a whole, is susceptible to damage.

1.1.9 **Physical Security.** Physical security is the protection of a facility by physical or psychological means against pilferage, theft, fire, and sabotage.

1.1.10 **Emergency Headquarters.** A predesignated alternate site at which top management would operate in the event of a national emergency or disaster.

1.1.11 **Alternate Reporting Centers.** Predesignated locations, approved by the top management of a company, where facility employees will assemble in event of emergencies.

1.1.12 **Emergency Operations.** Limited to wartime conditions.

1.1.13 **Normal Operations.** All periods of time except wartime conditions.

1.1.14 **Mutual Aid.** In disaster planning and in planning emergency operations, an organization of manpower, equipment and materials whereby an affected company would receive help from another company in the communications industry in restoring essential service.

1.1.15 **Mobile Service Equipment.** That portable equipment, with or without supplies, owned or leased by a communications company, which is designed for use in maintenance or emergency restoration of service and for construction purposes, and including also supervisory vehicles.

1.1.16 **Sabotage.** The willful act or attempt to destroy, injure, or make in a defective manner war material, war premises, or war utilities with intent to injure, interfere with, or obstruct the National defense of the United States. (U.S. Code, Title 18.)

1.1.17 **Espionage.** The obtaining, receiving, communicating and delivering, or attempt thereof, of information respecting the national defense with intent or reason to believe the information will be used to the injury of the United States or to the advantage of a foreign nation. (U.S. Code, Title 18.)

1.1.18 **Subversive Activity.** "Subversive activity in this country derives from conduct intentionally destructive of, or inimical to, the Government of the United States—that it seeks to undermine its institutions, or distort its functions, or impede its projects, or to lessen its efforts, the ultimate end being to overturn it all. Such activity may be open and direct as by effort to overthrow, or subtle and indirect as by sabotage." (House Report No. 448, 78th Congress, 1st Session.)

1.1.19 **Emergency.** A sudden unexpected happening or development of pressing necessity requiring prompt, rapid and efficient action or counteraction.

Section 2

Industrial Defense Program

2.1 PURPOSE AND SCOPE.

2.1.1 **General.** The purpose of industrial defense in the communications industry is to reduce vulnerability; to prevent or minimize the effects of damage resulting from natural disaster and enemy attack; and to prevent or protect against sabotage, espionage, subversive activity, and inimical acts.

2.1.2 **Company Level.** Industrial defense at the company level of any communications common carrier (telephone, telegraph, radio and cable), includes that planning and direction which is necessary to insure the adequacy of a comprehensive company industrial defense program. This program is implemented at individual facilities within each company. Such a program would include:

2.1.2.1 Physical security policy.

2.1.2.2 Company policies pertaining to continuity of personnel.

2.1.2.3 Company policies concerning civil defense measures.

2.1.2.4 Company plans pertaining to continuity of service.

2.1.3 **Facility Level.** Industrial defense at the facility level within the communications industry includes:

2.1.3.1 The implementation of company plans and policies referred to above.

2.1.3.2 The identification and reduction of vulnerability of critical areas within the facility.

2.1.3.3 Facility physical security measures.

2.1.3.4 Fire protection measures.

2.1.3.5 Facility civil defense measures.

2.2 INDUSTRIAL DEFENSE COORDINATOR.

2.2.1 **Designation.** Each company in the communications industry should appoint an Industrial Defense Coordinator to be responsible for industrial defense matters at the company level. A facility coordinator should also be designated to be responsible for industrial defense matters at the facility level. When appropriate, a facility coordinator may be responsible for industrial defense activities at more than one facility, such as unattended stations or very small

facilities. The duties of a company or facility Industrial Defense Coordinator may not require full time. If other duties are assigned, the industrial defense duties should be regarded as an important part of the overall responsibilities of the Industrial Defense Coordinator.

2.2.2 **Authority and Functions.** The company and facility defense coordinator should be authorized to perform duties which include, but are not limited to, responsibilities for:

2.2.2.1 Direction or supervision of all industrial defense activities throughout the company or within a facility.

2.2.2.2 Participation in all industrial defense surveys.

2.2.2.3 Recommending to top management, plans, policies, and measures for improving the physical security of the company or facility.

2.2.2.4 Direction or supervision of periodic tests of company and facility emergency operations plans.

2.2.2.5 Supervision of industrial defense education systems and activities. (See 2.4 below.)

2.3 SURVEY AND REPORT RECOMMENDATIONS.

2.3.1 The recommendations resulting from Industrial Defense Surveys will generally fall into two categories:

2.3.1.1 Those for planning and implementation of plans at both the company and facility level.

2.3.1.2 Those requiring the expenditure of funds for the procurement, installation, and maintenance of protective equipment and training, supervision and use of guards.

2.4 INDUSTRIAL DEFENSE EDUCATION.

2.4.1 Industrial defense education at the facility level will include, but should not be limited to the:

2.4.1.1 Development of an awareness, on the part of each employee, of the importance of promoting security and protection of the facility.

2.4.1.2 Development of an understanding, by each employee, of his industrial defense responsibilities for maintaining security within an operating area, specifically, any area designated as a Critical Area. These responsibilities include, among others, the challenging and reporting by employees of persons whose presence on the premises is not authorized.

2.4.1.3 Each employee should be informed that the Federal Bureau of Investigation has jurisdiction for investigating matters of sabotage. Any incident of actual or suspected sabotage should be reported promptly to the nearest office of the FBI.

2.4.1.4 Each employee should be instructed to report promptly to the Industrial Defense Coordinator the presence of any device which is believed to be intended for sabotage. The nearest FBI office should be notified immediately.

2.4.2 Provision for the immediate indoctrination of new employees should be made at the facility level.

2.5 TESTS.

2.5.1 Written plans such as for evacuation, movement to shelters, and fire drills should be periodically tested to insure that all participants become thoroughly familiar with their specific duties, and to eliminate discrepancies which may be found to exist. Following such tests, plans should be revised as necessary and succeeding tests should be redesigned accordingly.

2.5.2 The testing of corporate relocation plans and any other phase of the overall corporate disaster plan should be conducted periodically.

Section 3

Criticality and Vulnerability

3.1 FACILITY CRITICALITY.

3.1.1 General. The over-all criticality of any communications facility within the Industrial Defense Program is established prior to the survey by the fact that the facility concerned is of vital importance to continuity of communication service. Key Facility listings within the communications industry are jointly determined by the Department of Defense and industry representatives, and each communications facility to be surveyed is of high critical nature from the national defense viewpoint.

3.2 CRITICAL AREAS. Some facilities will have areas which are critical to continuity of service. Such areas will be considered as "critical areas" upon advice of local personnel and should be afforded appropriate protection.

3.2.1 Noncritical Equipment. Loss of some equipment in operating areas within a facility could cause an interruption in service, measured in terms of minutes. Availability of equipment for immediate replacement or the industrial flexibility to immediately re-route, reduces the criticality of some facilities to a point where only minimum physical security measures may be needed.

3.2.2 Management Responsibility. Defense Coordinators should be prepared to present to surveying personnel their designation of critical areas within their facilities.

3.3 FACILITY VULNERABILITY.

3.3.1 Considerations.

3.3.1.1 During normal operations most all communications company employees working within a facility have access to any part thereof on a Departmental basis except at locations where classified projects impose restrictions.

3.3.1.2 During emergency operations many persons presently employed would be given limited access to critical areas, since access to such areas would be on an actual need basis.

3.3.1.3 Physical separation of critical areas within a facility decreases vulnerability.

3.3.2 **Vulnerability Determination.** In determining vulnerability of a critical area within a facility, the primary factors are:

3.3.2.1 Accessibility to the critical area from within or from outside of the facility.

3.3.2.2 Possibility of damage to the critical area as a result of flood.

3.3.2.3 The degree to which a critical area could be damaged by fire, explosion, or other cause including that which may result if an adjacent structure is destroyed or damaged.

3.4 VULNERABILITY REDUCTION.

3.4.1 **Phases.** Vulnerability reduction can be achieved in two separate phases:

3.4.1.1 Limiting access to all areas to personnel who have an actual need for same.

3.4.1.2 Reducing the effects of damage (resulting from theft, fire, flood, sabotage, or explosion).

3.4.2 **Security Inspection.** Periodic security inspections should be made during normal operational periods by the person responsible for defense coordination.

Section 4

Physical Security

4.1 PHYSICAL SECURITY PLANNING.

4.1.1 General Considerations. The physical security problem is affected by:

4.1.1.1 The criticality of the facility.

4.1.1.2 The physical arrangement of the facility.

4.1.1.3 The vulnerability of the facility.

4.1.1.4 Geographical location of the facility.

4.1.1.5 Number of people employed at the facility at various times of the day and night.

4.1.1.6 Exposure to adjacent or nearby hazards.

4.1.2 Physical Security Estimate. Prior to the development of a physical security plan, it is necessary to make a complete physical security estimate of the facility involved. The underlying concept in such an estimate is to regard the facility from the viewpoint of the intruder. It is necessary to determine the areas which an intruder would attempt to put out of commission, his avenues of approach and his method in neutralizing his objective. This estimate, therefore, will illustrate:

4.1.2.1 Critical areas as viewed by the opposition.

4.1.2.2 Vulnerability of such areas as illustrated by existing hazards.

4.1.3 Economic Considerations. Cost is a vital consideration in the implementation of any physical security recommendations. Such recommendations should be designed to insure adequate security at minimum expense. During periods of normal operations, it is sometimes necessary to place physical security aids into use because long procurement lead time in time of emergency will preclude acquisition when needed. In time of emergency, these same considerations should apply, with the exception that lead time for new equipment should be even further reduced.

4.1.4 Degrees of Physical Security. Physical security measures recommended by survey personnel will vary, not only from one facility to another, but within areas of any one facility. To assist survey

personnel and defense coordinators in establishing an appropriate degree of security for and within facilities in the communications industry, *full consideration should be given* to the elements contained in Section 3 of these Criteria.

4.1.5 **Physical Security Plan.** A physical security plan consists of a systematically outlined program, designed to reduce existing hazards and thereby reduce the vulnerability of the facility to a point where success on the part of the intruder is unlikely. This plan may be in *any format* desired by management, as long as all essential areas and measures as well as directions are included.

4.2 PERIMETER BARRIERS.

4.2.1 **General.** A perimeter barrier is that device which defines the limits of the facility area. Such a barrier can, if facility property includes space adjacent to buildings, be defined by a fence surrounding the various facility structures. If however, the facility boundary is defined by the walls of a building, then that entire building becomes the perimeter barrier, and must be treated as such.

4.2.2 **Purpose.** The primary purpose of perimeter barriers is to restrict or delay access to critical areas by unauthorized persons. Perimeter barriers, in order to be effective, should accomplish the *following*:

4.2.2.1 Define the perimeter of the facility or controlled area.

4.2.2.2 Create a physical and psychological deterrent to persons attempting or contemplating unauthorized entry into the area.

4.2.2.3 Delay intrusion, enabling security personnel to detect the intruder because of the time element involved.

4.2.2.4 Facilitate the effective and economical use of guard forces, if applicable.

4.2.2.5 Direct and channel the flow of personnel and vehicles through designated places of entry as a measure of control.

4.2.3 **Effectiveness of Perimeter Barriers.** A perimeter barrier by itself serves no physical security purpose unless it is adequately backed up by other security aids such as lighting, intrusion detection devices and guards. The use of a combination of these aids depends in each case upon the facility concerned and degree of physical security required.

4.2.4 **Fences—General.** If fences are used as a portion or all of the perimeter barrier, they should be of sufficient durability of design and height to:

4.2.4.1 Render climbing difficult.

4.2.4.2 Prevent bending so as to facilitate entry.

4.2.4.3 Prevent entry through space between the bottom of the fence and the top of the ground.

4.2.5 **Fence Specifications.** Fence should be a minimum of seven feet in height, topped with a 45 degree outward and upward extending arm bearing three strands of barbed wire stretched taut and so spaced as to increase the vertical height of the fence by approximately one foot. Where property lines and local laws prohibit the outward extension of overhangs, the top guard may be extended inward. Where use of such top guard is not possible, the fence should be extended to a height of eight feet. The type of construction found in chain-link fence is desirable.

4.2.6 **Building Walls.** Walls, floors, roofs, and dikes, when serving as perimeter barriers, should be of such construction and so arranged as to provide uniform protection equivalent to that provided by fencing as specified above. Where buildings form a part of the perimeter barrier, fence height should be increased 100% at the point where the fence joins the building wall. The increase should be gradual from a point on top of the fence not less than ten feet from the wall. Where building wall surfaces are smooth and the utilization of trucks (on-loading or off-loading up against the building) do not present a hazard, fence height need not be increased.

4.2.7 **Openings in Perimeter Barriers.** Openings in the perimeter barrier should be kept to a minimum. They should be constantly guarded, locked, or otherwise secured. Fences should be provided with culverts, troughs, or other openings, where necessary to prevent washouts in the perimeter barrier and to permit carry-off of excessive drainage and small streams. Such openings, when larger than 96 square inches in area, should be provided with physical barriers equivalent in protective capabilities to those of the perimeter barrier itself, and so designed as to minimize impedance to water run-off.

4.2.8 **Security of Gates and Doors.** When not in active use and controlled by guards, gates and doors in the perimeter barrier should be locked and frequently inspected by patrols. Locks should be changed from time to time. Security for the keys of such gates and doors should be the responsibility of the Defense Coordinator and may be sub-delegated to the chief of guards or other designated member of the guard force, if applicable. An effective key control (check-out) system should be established. Seals placed on gates or doors in conjunction with locks will greatly increase the security. For physical security purposes a lock and key change possibility should be considered. Doors should have hinges arranged so as to prevent removal of hinge pins.

4.2.9 **Security of Windows.** Windows and other openings which penetrate the perimeter barrier and have an area of 96 square inches or greater should be protected by securely fastened bars, grills, or other equivalent means when located less than 18 feet above the

level of the ground outside the perimeter barrier or less than 14 feet from structures outside the perimeter barrier.

4.2.10 **Security of Utility Openings.**

4.2.10.1 **Sewers, Intakes and Tunnels.** Sewers, air and water intakes, exhaust tunnels, and other utility openings which penetrate the perimeter barrier and have a cross-section area of 96 square inches or greater should be protected by bars, grills, water-filled traps, or other structural means providing security equivalent to that of the perimeter barrier. Manhole covers (tunnel type ducts) within or adjacent to the perimeter barrier should be secured by locks.

4.2.10.2 **Coal Chutes and Fuel Tank Intakes.** Where utility openings such as intakes for coal chutes and auxiliary fuel tanks are located outside the perimeter barrier, such openings should be locked. During delivery of oil or coal through such openings in the barrier, the delivery should be supervised by facility personnel so as to preclude the introduction of damaging material by supplier or would-be supplier personnel.

4.2.11 **Manholes.** Central office and other important manhole covers should be secured by locking such covers during normal as well as emergency conditions.

4.2.12 **Clear Zones.** Where a perimeter barrier is located outside or around existing structures, clear zones should be maintained to facilitate observation and preclude obstructions near or at the barrier. An internal clear zone of 10 feet or greater should be maintained at all times. Although a 20 foot outside clear zone is desirable, such clear zones are generally not feasible when the facility is located in an urban area. It is, however, necessary that liaison be established with local authorities, adjacent property owners, and utility companies to insure the removal of climbing devices such as utility poles, trees and storage of equipment from the area immediately adjacent to the barrier. When the building of the facility is coincidental with the perimeter barrier, adjacent buildings should be carefully checked to insure that access to the roof or windows of the facility (at any given height), cannot be effected from the adjacent structure. Such a condition may necessitate the barring of windows above the first floor and the erection of fencing on top of the roof of the facility concerned.

4.2.13 **Maintenance.** Perimeter barriers serve no useful purpose unless they are completely checked for damage or deterioration at least on a monthly basis by local maintenance crews. Repairs should be handled on a priority basis and guards as well as defense coordinators should be constantly alert to check for evidence of tampering and report such incidents on an immediate basis.

4.2.14 **Signs.** Perimeter barriers may be posted with signs reading

"Private Property No Trespassing," if desired. Such signs serve legal rather than security purposes. From a security viewpoint, the only signs which should be used as desired are statements to the effect:

4.2.14.1 "Authorized Personnel Only."

4.2.14.2 "Entry Constitutes Permission to be Searched." The use of this sign is contingent upon local laws. Prior to use of this sign, the company counsel should be consulted.

4.2.14.3 Warning signs reading "Admittance to Authorized Personnel Only," should be conspicuously posted at entrances to unlocked critical areas. If a critical area is kept locked, warning signs need not be posted. Signs identifying areas as "Critical Areas" will not be used.

4.3 IDENTIFICATION AND CONTROL.

4.3.1 **General.** Identification and control of personnel and vehicles which are allowed access to the critical areas of the facility is a vital portion of the security plan. The degree of control is directly related to the degree of physical security required. Recommendations for types of identification system should constantly reflect this premise. At the same time, any identification system used must permit optimum movement with minimum control to insure that physical security does not interfere with the operational mission of the facility. It is, therefore, necessary that any identification and control system used:

4.3.1.1 Provide a ready means of positive identification of both personnel and vehicles authorized access to critical areas of the facility.

4.3.1.2 Facilitate the control of ingress, egress and circulation of personnel to, from, and within the critical area, commensurate with operational requirements.

4.3.1.3 Provide a visible means for rapid recognition of any limitations of movement or access imposed within the facility.

4.3.2 **Personnel Clearance.** Where classified Defense information is utilized by the facility, the personnel clearance program must adhere to the provisions of the Armed Forces Industrial Security Regulation.

4.3.3 **Company Background Checks.** Industry should conduct reasonable checks of all new employees. These checks are primarily designed to ascertain the applicant's suitability for employment and have long been a standard practice with American industry, consistent with fair employment practices. These checks, or variations thereof, may include, but not necessarily be limited to:

4.3.3.1 Date and place of birth.

4.3.3.2 Citizenship.

4.3.3.3 Applicant's military discharge certificate, if applicable.

4.3.3.4 Criminal records, where practicable.

4.3.3.5 Employment references.

4.3.4 **Vehicle Registration and Control.** Trucks and conveyances which must have access to a point within the perimeter barrier should be restricted to the use of a service gate where they are subject to inspection by guard personnel. If the building is coincidental with the perimeter barrier, and loading or unloading operations take place on ramps or loading platforms at the building, it is necessary that packages, crates, and other equipment should be spot checked by guards or designated facility employees. To facilitate control, a truck register should be maintained and include information identifying the truck by license number and company, the signature of the driver, description of the load, and the date and time of both entrance and departure. During emergencies these measures should be extended to include actually checking the operator's license of drivers and helpers and utilize bills of lading or other such documents which will identify the driver and the helpers as being affiliated with the company reputedly handling the shipment. Under these circumstances, full checks of incoming and outgoing material should be made.

4.3.5 **Outside Suppliers.** Soft drink dispensers and other vending machines utilized by the facility should be located sufficiently distant from critical areas, so as to preclude unauthorized access and damage. This also applies to concessionaires who operate cafeterias within the facility. *It may be necessary to provide escorts for such vendors* and suppliers as well as concessionaires.

4.3.6 **Personnel Identification—Normal Operations.** During periods of normal operations, any identification is adequate if it controls access of authorized personnel to critical areas.

4.3.7 **Personnel Identification—Emergency Operations.** During periods of emergency operations, a comprehensive identification system should be used. This identification system should consist of a tamper proof type badge or pass which will permit close control of access to facilities. These identification media should contain:

4.3.7.1 A suitable photo of the individual.

4.3.7.2 Last name and initials.

4.3.7.3 A color strip or code where appropriate.

4.3.7.4 Date of birth.

4.3.7.5 Company name.

4.3.8 Badges, if used, should be worn by all employees at all times while employees are inside controlled areas.

4.3.8.1 **Wearing Identification Media.** To facilitate rapid and accurate identification of personnel having access to controlled areas, these badges, if used, should be worn in a uniform place, depending upon the desires of the defense coordinator.

4.3.8.2 **Clearance Data on Badges.** At no time should these badges reflect the degree of clearance for access to classified material on the part of the bearer. Any card, pass or badge reflecting the bearer's clearance status is not authorized by the Department of Defense and should not be honored.

4.3.8.3 **Electro-magnetic Badges.** The utilization of electro-magnetic badge system should be explored and if, from an economy viewpoint, installation of this system is feasible, appropriate recommendations should be made.

4.3.8.4 **Badge Preparation and Control.** General control of procedures and practices for issuance of badges and passes should be retained at the company level and be standardized throughout the company.

4.3.8.5 **Employee Briefing.** To insure the effectiveness of the identification media, it is necessary that new employees are briefed in an orientation, to include:

4.3.8.5.1 Description of the identification media used and the authorization and limitations of the bearer.

4.3.8.5.2 The mechanics of identification at time of egress and ingress to the facility.

4.3.8.5.3 Details of how, when, and where badges, if used, will be worn.

4.3.8.5.4 Applicable laws pertaining to espionage, sabotage, and subversion.

4.3.8.5.5 Individual employee responsibilities in identifying fellow employees working in the same area.

4.3.9 **Visitor Control.**

4.3.9.1 **Registration.** Where practical, all visitors to critical areas should be registered.

4.3.9.2 **Types of Visitor Badges.** If badges are normally used at the facility, visitor badges of two types should be issued to such personnel.

4.3.9.2.1 Those visitors requiring escorts should have a badge, preferably of a predesignated color and should be escorted at all times while within the facility.

4.3.9.2.2 Visitors not requiring escorts should be given a different color badge and may have free access within the facility. This category would specifically apply to personnel from company headquarters.

4.3.9.3 **Types of Visitors.** All visitors, including inspectors, technical experts or representatives of government agencies, including the military, should be properly identified. Military or other government identification media are not to be utilized as a badge or pass authorizing access to any facility. No public visitations should be permitted to critical areas. Under no circumstances will vendors, concessionaires or outside vendor suppliers have access to critical areas. Except as described in the following subsection, all visitors having need for access to critical areas should be escorted.

4.3.9.3.1 Visitors who are employees of outside contractors may repeatedly return to the facility for work on the premises for several days duration. Such visitors include plumbers, electricians and painters who frequently work in critical areas. Special consideration and careful attention should be given by the facility Industrial Defense Coordinator when such work is anticipated. It may be necessary for facility coordinators to consult with Company Industrial Defense Coordinators on the need for obtaining reasonable checks on outside contractor employees from their respective employers. (See Section 4.3.3.)

4.4 PROTECTIVE LIGHTING.

4.4.1 **Application.** Perimeter barriers and adjacent areas should be lighted during hours of darkness and periods of low visibility. The intensity of light should be sufficient to permit the detection of an intruder. The beam spread of protective lighting should cover completely the area between light poles.

4.4.2 **Glare Lights.** Glare projection lights serve to blind the intruder who approaches the perimeter from the outside. Such lighting should be so directed not to strike the eyes of guards or to create a hazard to traffic on a public highway.

4.4.3 **Use at Gates.** Main gates at entrances should be lighted sufficiently to insure proper identification of personnel and examination of credentials.

4.4.4 **Special Lighting Systems.** Certain communication facilities may be operated in a manner to attract minimum attention and may be provided with a protection lighting system which is normally not in use, but which is capable of being instantly used in the event of an emergency or suspicious occurrence near the perimeter barrier of the facility.

4.4.5 **Auxiliary Power.** The protective lighting system should be capable of operating from auxiliary power in the event of failure of the normal power source.

4.5 PROTECTIVE ALARMS AND INTRUSION DETECTION SYSTEMS.

4.5.1 **Use.** Consideration should be given to the maximum use of

alarm and intrusion detection systems as an essential adjunct to the effective utilization of guard forces and the establishment of an economical physical security program.

4.5.2 **Availability of Technical Data.** Technical data on alarm systems and intrusion detection devices may be obtained from Department of Defense survey personnel. Performance data and guidance regarding specific utilization of devices under given conditions at the facility concerned may also be obtained from survey personnel. The Department of Defense does not, however, endorse specific alarm systems, detection devices or other alarm manufacturers' products.

4.6 PROTECTION OF COMPANY INFORMATION. Certain information, proprietary to communication companies, is of value to saboteurs and espionage agents. This information should be safeguarded by management. Before releasing proprietary information, management should be assured that the recipient has a "need-to-know," will not further disseminate the information, and will provide proper safeguards for the information while in his custody.

4.6.1 These data include, but are not limited to:

4.6.1.1 **Prints** of facilities; of operating equipment.

4.6.1.2 **Diagrams** of operating equipment locations; of circuit layouts (local as well as inter-state and international); of underground cables in metropolitan areas.

4.6.1.3 **Data** for priorities system to be used in an emergency; on critical area designations; on company and facility pass blanks and code numbers; on any item or material considered to be critical or in short supply.

4.6.1.4 **Plans** on expansion and circuit re-routing; on company and facility industrial defense except in generalized terms; on company or facility industrial security.

4.7 GUARD FORCE.

4.7.1 In determining whether a guard force is needed at a certain facility, the following factors should be considered:

4.7.1.1 Size, location, and arrangement of facility.

4.7.1.2 Type of work performed—criticality.

4.7.1.3 Importance, classification, and vulnerability to damage of materials, data and equipment involved.

4.7.1.4 Effectiveness of mechanical security measures in effect and whether these can be supervised adequately by civil police or commercial protection organizations.

4.7.2 If a determination is made that a guard force is needed, the provisions of the Department of Defense "Standards for Plant Protection" should be used as a reference guide for such elements as guard qualifications, organization, duties and training.

Section 5

Fire Protection

5.1 INSURANCE INSPECTORS' REPORTS. Copies of fire insurance inspectors' reports will be made available to surveying officers at the company level. Specific recommendations therein will be reviewed at the facility.

5.2 ALARMS. Communication facilities normally have local internal alarms as well as those tying in with municipal fire departments. Such alarms should be checked for operational readiness. Employee response to alarms should also be checked in the event the system is activated.

5.3 LIAISON. Inasmuch as the use of water for fire fighting purposes is generally not desirable at communication type facilities, it is necessary that facility defense coordinators establish liaison with local fire departments to inform such organizations of the specific needs and requirements of the facility. This will preclude damage resulting from the use of water at communication facilities.

5.4 AUXILIARY FIRE FIGHTING. Employees of a communications facility should be organized into an auxiliary fire section, depending upon the physical layout of the building. Employees should be thoroughly indoctrinated in the use of available equipment, its location, and their specific action in the event of an alarm.

5.5 FIRE DRILLS. To test the adequacy of fire regulations and training, periodic fire drills should be conducted.

5.6 FIRE EXTINGUISHERS. Fire extinguishers should be checked frequently within a facility to insure that the material normally contained in the extinguisher has not been tampered with or replaced with substitutes.

Section 6

Continuity of Management and Personnel

6.1 GENERAL. Material contained in this section should serve as a guide in the development of this element of the Program by top management. In such development, it is suggested that consideration be given to:

6.1.1 **Emergency Succession.** Establishment of position sequence assignments, emergency functions of surviving successors, and selection of emergency personnel from different geographical locations.

6.1.1.1 Legal factors and board of directors approval where appropriate.

6.1.1.2 Emergency succession of personnel to key operational positions.

6.1.2 **Emergency Headquarters.** Designation of emergency or alert headquarters furnished with minimum equipment for operation by an emergency management team.

6.1.2.1 Criteria for locations could include, but not necessarily be limited to:

6.1.2.1.1 A site outside of a critical target area.

6.1.2.1.2 A site sufficiently close to a community to insure availability of transportation, communications and housing for personnel.

6.1.2.1.3 The possibility of use of an existing installation of the company, recognizing security requirements and accessibility.

6.1.2.1.4 Consideration of adequate shelter areas for protection of personnel against fall-out.

6.1.3 **Alternate Reporting Centers.** Consideration of emergency centers for employees at the company level.

6.1.3.1 Selection of sites and facilities as in Paragraph 6.1.2 above.

6.1.3.2 The provision of duplicate records as may be required.

6.1.3.3. Additional equipment at the alternate reporting centers may include emergency medical supplies, and radiation monitoring equipment, as such equipment becomes available.

6.1.3.4 Movement of mobile service equipment to the alternate reporting center or other appropriate locations before or after an alert.

6.1.4 Skill Inventory. Consideration of the availability of duplicate personnel records of major and secondary skills of employees who may report to alternate reporting centers.

6.1.5 Recall. Consideration of the availability of lists to facilitate the recall of local retired employees where practicable.

6.1.6 Personnel Records. Consideration of the practicability of retaining records at alternate company headquarter locations of all personnel expected to report to alternate reporting centers.

Section 7

Continuity and Restoration of Essential Service

7.1 POWER. It is desirable that provisions be made at the facility level to insure the availability of sufficient alternate power necessary for essential operations for a period determined by the maximum probable disruption. In the provision of alternate power equipment consider the availability of such items of supplies as oil, coal, gasoline, and water.

7.2 SUPPLIES. All facilities in the communications industry maintain a limited stock of replacement parts for essential equipment and machinery. Major items are generally obtained from readily available manufacturers in relatively short periods of time. During emergency operations, transportation of such equipment will become critical. Planning should, therefore, include provisions which would insure the availability of sufficient supplies to sustain minimum operations notwithstanding loss of transportation, and probable damage to critical equipment. The storage of such supplies should be sufficiently adequate to insure minimum damage from the effects of blast, flood, and fire. Storage sites within the facility should be periodically checked to minimize the possibility of tampering or theft.

7.3 MINIMUM OPERATIONS FROM SHELTERS. Provisions should be made to enable the facility to communicate from shelter locations to company relocation and control sites. Wherever possible, intra-company communications should be provided at existing shelters.

7.4 MOBILE EQUIPMENT. Within the communications industry, restoration of essential service will depend in large part upon the rapid dispatch of mobile service equipment to designated locations during the immediate post emergency period, including the crossing of state boundaries. Plans should, therefore, include implementing provisions for dispersal of mobile service equipment. Where this is not possible, arrangements should be made to insure the rapid dispersal of mobile equipment to relocation sites immediately upon receipt of the earliest warning. In the event of an emergency without warning, operators of mobile equipment should be instructed to report to predesignated relocation sites as expeditiously as possible and should be thoroughly familiar with routes to such locations.

7.4.1 Top management within the communications industry has established working mutual aid agreements within the industrial complex. These agreements are considered to be sufficient and are not further elaborated upon in these Criteria.

Section 8

Civil Defense Measures

8.1 LIAISON.

8.1.1 **Company Level.** It is necessary that each company establish liaison with local, state, and federal civil defense directors and administrators for the purpose of:

8.1.1.1 Establishing company civil defense plans.

8.1.1.2 Coordinating company civil defense tests with state and federal alert exercises, if applicable.

8.1.1.3 Obtaining civil defense assistance to insure rapid and uninterrupted movement of communications equipment and personnel during civil defense emergencies.

8.1.1.4 Establishing procedures to insure civil defense support and debris clearance at locations where access to communications equipment is necessary in post disaster periods.

8.1.1.5 Taking necessary action to assure company liaison with civil defense control centers.

8.1.2 **Facility Level.** It is of equal importance that local facilities establish liaison with municipal civil defense directors in consonance with company plans. The primary purpose of such liaison is to effect coordination and obtain guidance on matters referred to in Paragraph 8.1.1 above, as they may apply in each individual location.

8.2 RADIATION MONITORING. When tested and accurate equipment is available and practicable, radiation monitoring planning seems desirable at the company level.

8.3 EMPLOYEE DUTIES.

8.3.1 In order to insure the continuity of essential service during a civil defense emergency, it is necessary that management designate those categories of communication employees to be advised of their first priority of operational responsibility.

8.4 SHELTERS. Defense Coordinators at the Company level shall arrange for the designation, marking, and equipping of existing areas to be used as shelters in the event of emergency. The designation of existing structures and equipment for same should be in consonance with applicable publications of the Office of Civil and Defense Mobilization.

8.5 WARDENS. Facility defense coordinators will establish a warden type organization for each facility. The primary purpose of this organization is to interpret a warning and insure the orderly

movement of personnel to and from designated shelters in the event of an emergency. Wardens should be further responsible for insuring orderly and systematic evacuation of the facility, or portion thereof, as the need arises.

8.6 RESCUE. Depending upon the need and type of construction of each facility, light and heavy rescue squads should be trained and equipped through existing civil defense channels.

8.7 MEDICAL. Medical supplies and equipment should be available in or near shelters within each building. Equipment should be of sufficient quantity to cope with the maximum number of facility employee casualties which may be anticipated in the event of disaster.

U.S. GOVERNMENT PRINTING OFFICE: 1960

GPO 920700